SEMARAK ILMU PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Chinese Remainder Theorem-Based Encoding of Text to Point Elliptic Curve Cryptography

Josepha Menandas J.[1,*], Mary Subaja Christo[1]

[1] School of Computing, SRM Institute of Science and Technology, Kattangulathur, Chennai, India

ARTICLE INFO	ABSTRACT
Article history: Received 21 August 2023 Received in revised form 6 March 2024 Accepted 11 March 2024 Available online 25 June 2024 ***Keywords:*** Elliptic curve cryptography; Chinese remainder theorem; Confidentiality; High security; Prime field; Encryption; Decryption	One of the most crucial requirements in this digital age is data security. The number of data usage increased drastically now a days, but how far the data is secured is the very big problem, though we have enough cryptographic algorithms for securing real time applications, but the level of the security against modern attacks is not determined. Elliptic Curve based Cryptography (ECC) is the most important cryptographic algorithm for confidentiality and authentication, providing high security level with small length keys when compared to other asymmetric algorithms like RSA, Diffie-Hellman, etc. The real time system usage of ECC is very less due to computational complexity. So, to increase the real time system usage we propose the novel method of combining the ECC with the Chinese Remainder Theorem (CRT), to reduce the larger values to the smaller one, so that the complexity of constructing ECC points can be reduced nearly 40% when compared to the existing ECC based algorithms. Also, its proved that the level of security getting increased and can be used as the fundamental component in real time communication system.

1. Introduction

Elliptic curve cryptography (ECC) is a type of public-key cryptography that is based on the mathematics of elliptic curves over finite fields. It provides a secure method for key exchange, digital signatures, and encryption.

In ECC, each user has a pair of cryptographic keys: a private key and a public key. The private key is kept secret and used for generating digital signatures or decrypting messages, while the public key is shared with others and used for verifying signatures or encrypting messages.

The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). The ECDLP states that given a point P on an elliptic curve and another point Q, it is computationally infeasible to find an integer k such that Q = kP, where k is the private key and Q is the public key.

ECC offers several advantages over other public-key cryptosystems, such as RSA:

* *Corresponding author.*
E-mail address: menandasjosepha@gmail.com

https://doi.org/10.37934/araset.47.2.148159

i. Security: ECC provides the same level of security as other public-key cryptosystems but with shorter key lengths. This results in faster computation and lower resource requirements.
ii. Efficiency: ECC operations, such as key generation, encryption, and decryption, can be performed with fewer computational resources compared to other algorithms, making it suitable for resource-constrained environments like mobile devices and embedded systems.
iii. Bandwidth and storage efficiency: ECC produces shorter key sizes, which results in smaller digital signatures, ciphertexts, and certificates. This makes ECC more efficient in terms of bandwidth usage and storage requirements.
iv. Future-proofing: ECC is considered more resistant to attacks from quantum computers compared to traditional public-key algorithms like RSA and DSA. This makes ECC a potential choice for long-term security.

ECC is widely used in various applications, including secure communication protocols like Transport Layer Security (TLS), digital signatures, key exchange protocols like Diffie-Hellman key exchange, and more in [5-10].

It's important to note that while ECC offers strong security, its implementation must be done carefully to avoid vulnerabilities. Keeping software and hardware up to date, using well-vetted elliptic curve parameters, and following best practices are crucial for maintaining the security of ECC systems. the importance of Elliptic Curve Cryptography lies in its ability to provide strong security, efficiency, scalability, and standardization for various cryptographic operations, including key exchange and digital signatures. Its small key sizes and computational efficiency make it particularly valuable in resource-constrained environments, while its wide adoption ensures interoperability and compatibility in modern cryptographic systems.

2. Related Work

2.1 Literature Review of Text to Point Mapping Process

Several attempts have been made to take advantage of the ECC's strength in a variety of public-key encryption activities, including confidentiality, authentication, integrity and nonrepudiation. Koblitz [11] presents an encoding a message to a point on an elliptic curve using a probabilistic approach that involves first turning the message into a string of numbers. The auxiliary base parameter 'k' is then multiplied by each number 'n', taken as the x-coordinate value and find possible y value which solves the elliptic curve equation. In [12], the ASCII cypher characters are utilised to locate the elliptic curve points while the Hill cypher method is employed to encrypt the message. [13] discusses a method for implementing message encryption using the ECC algorithm in which a character is transformed into a point on the curve by multiplying its ASCII value by the original affine point. The ElGamal elliptic curve encryption method is then used to encrypt this point. In [11], authors suggested employing mirrored elliptic curves to extend the Koblitz approach. it suggested the same Koblitz method with transposition technique. Before characters are mapped to the curve, propose the usage vector and XOR function on plaintext characters. This means that a polyalphabetic cypher will be produced by encrypting the mapped locations. The Koblitz method and the Time Dependent Multiple Random Cypher (TDMRC) code were suggested in [12] as a secure way to put plaintext on an elliptic curve. A quick mapping method utilising a non-singular matrix was suggested in [13]. In [14] provided a succinct overview of key exchange, encryption, and decryption using ECC. The authors used a mapping table to translate the ASCII value into an elliptic curve coordinate.

2.2 Elliptic Curve Cryptography

In ECC, the process of converting text to points on an elliptic curve involves a mathematical operation known as scalar multiplication of an elliptic curve. Here's a high-level overview of the steps involved:

i. Choose an Elliptic Curve: Select an appropriate finite field elliptic curve. The equation of the elliptic curve is $y^2 = x^3 + ax + b$, where a and b are constants specific to the curve.
ii. Define a Base Point: Select a point P on the curve called the base point or generator. This point should have a large prime order, meaning that when you repeatedly add it to itself, you eventually get the identity element (point at infinity).
iii. Convert Text to a Numeric Representation: Encode the text you want to encrypt into a numeric representation. This step can involve various encoding schemes, such as ASCII or Unicode, depending on the specific implementation or requirements.
iv. Generate a Private Key: Choose a random integer k as your private key and the key value should be in the range between 1 and the order of the high base point.
v. Perform Scalar Multiplication: Multiply the base point P by the private key k. Scalar multiplication involves adding the base point to itself k times. This operation results in a new point on the elliptic curve, which is your public key [14].

The output of the resulting point is the public key corresponding to the private key. It can be represented as coordinates (x, y) on the curve.

It's important to note that the conversion of text to points is only a part of the ECC encryption process [15]. With the help of elliptic curve mathematical properties, provide secure key exchange, digital signatures, and encryption. The encryption process typically involves additional steps, such as generating a shared secret using the recipient's public key and performing symmetric encryption with that shared secret [16].

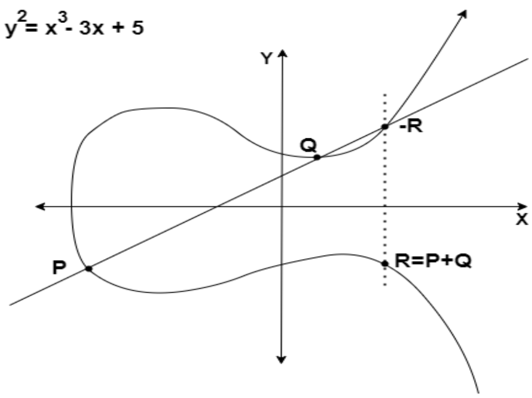

Fig. 1. Elliptic Curve Points Addition. (R=P+Q)

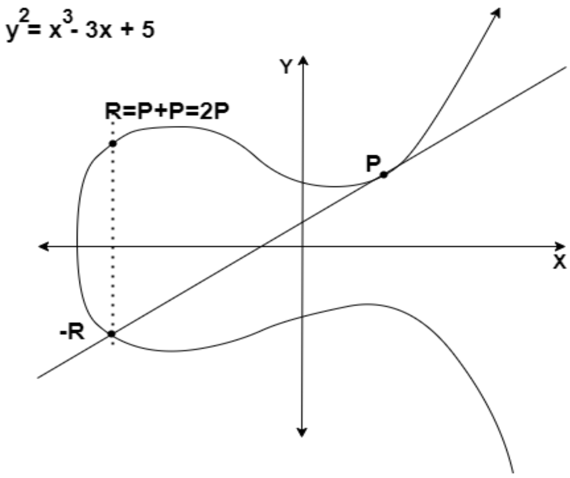

Fig. 2. Elliptic Curve Points Doubling(R=P+P=2P)

2.3 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is a fundamental theory in modular arithmetic and the most important number theory. It gives a deterministic step to solve a problem of congruences or modular equations with pairwise coprime moduli.

Let's say we have a system of congruences:

$$x \equiv a_1 \ (mod \ m_1) \tag{1}$$

$$x \equiv a_2 \ (mod \ m_2) \tag{2}$$

...

$$x \equiv a_n \ (mod \ m_n) \tag{3}$$

where a_1, a_2, ..., a_n are given remainders, and m_1, m_2, ..., m_n are pairwise coprime moduli (i.e., the greatest common divisor of any two moduli is 1).

The CRT states that there exists a unique solution for x modulo M, where M is the product of all the moduli:

$$M = \ m_1 \times m_2 \times \cdots \cdots \cdots \times m_n \tag{4}$$

The theorem provides a constructive method to find this solution, known as the Chinese Remainder Theorem algorithm. Here's a simplified version of the algorithm:

Compute $m_1, m_2, \cdots \cdots \cdots m_n$ where $M = \ m_1 \times m_2 \times \cdots \cdots \cdots \times m_n$ with no common multiplicative factors of m_i.

For each congruence $x \equiv a_i \ (mod \ m_i)$, compute the value b_i such that

$$b_i \equiv \left(\frac{M}{m_i}\right) mod \ m_i. \tag{5}$$

This can be done using the extended Euclidean algorithm or by using modular inverses. Calculate the solution x by taking the sum of the products of a_i and b_i modulo M:

$$X = (a_1 \times b_1 \times \frac{M}{m_1} + a_2 \times b_2 \times \frac{M}{m_2} + \cdots .. + a_n \times b_n \times \frac{M}{m_n}) mod\ M \tag{6}$$

The value of x obtained in step 3 is the unique solution to the system of congruences. The Chinese Remainder Theorem has various applications in number theory, cryptography, and computer science. It is particularly useful for solving modular equations in cryptographic protocols, optimizing computations in certain algorithms, and finding solutions in modular arithmetic systems [18-21].

3. Proposed Methodology

3.1 Architectural Framework of Proposed Method

Figure 3 shows the overall architectural frame work of the proposed methodology, which consists of four primitive functionalities. They are:

i. Text to Elliptic Curve Point Mapping
ii. ECC-CRT Encryption
iii. ECC-CRT Decryption
iv. Reverse Mapping of Elliptic Curve Point to Text

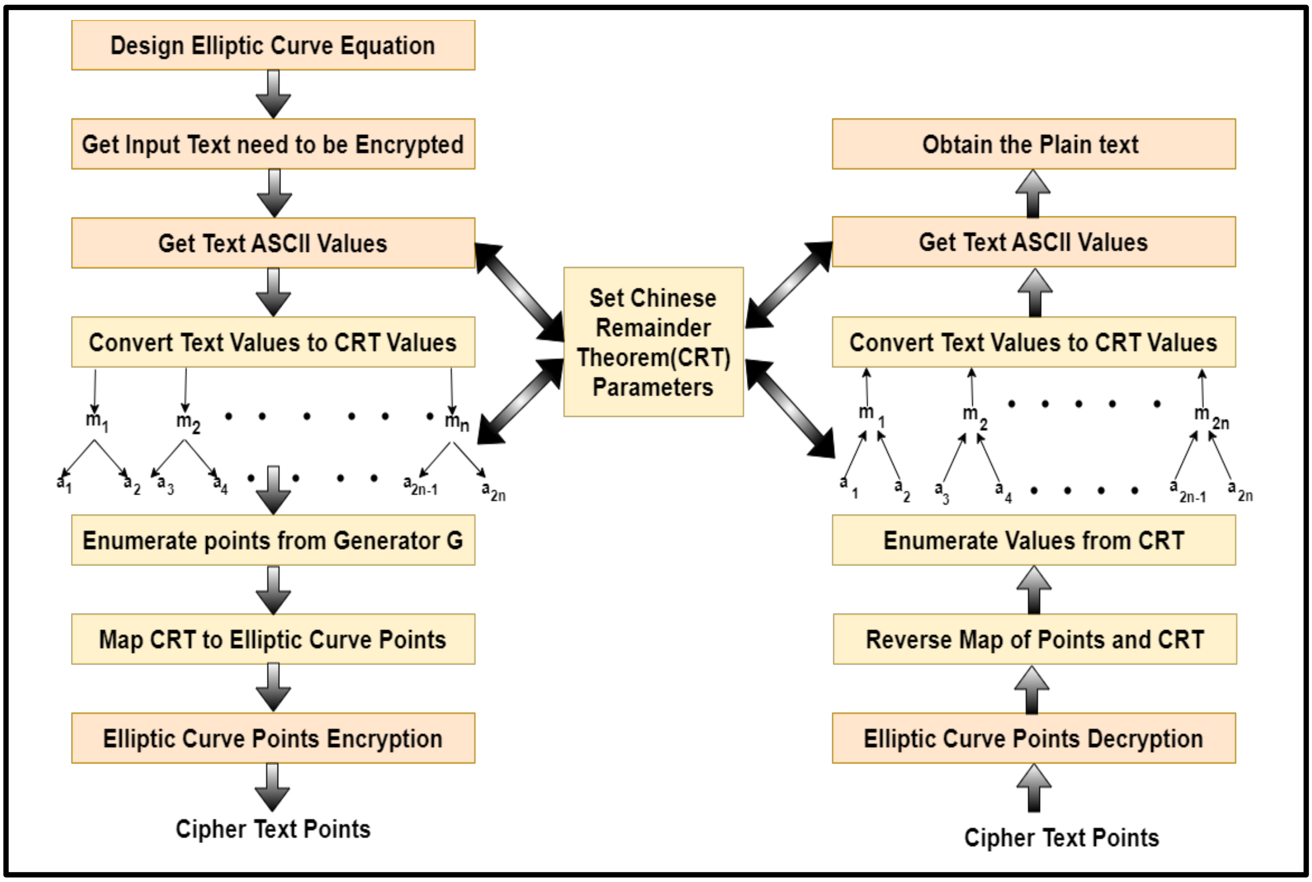

Fig. 3. Architectural framework of Proposed ECC-CRT algorithm

3.2 Setting of Prime Modules of Chinese Remainder Theorem

The ASCII value of every character is obtained then, every ASCII values are converted to pair of values based on the multiplicative prime moduli $(m_1, m_2)\ of\ M$ of the Chinese Remainder Theorem. Further, every CRT values are converted to Elliptic Curve Points, based on the Elliptic Curve Generator function. The following algorithm shows the conversion of text to ECC points using CRT.

3.3 Text to Elliptic Point Conversion Algorithm

Global parameters: $E_P(a,b), G, N, M, m_1, m_2, T$ where,
P – prime number
a, b are integers satisfying the equation(#)
G – Generator points ∈ $E_p(a,b)$
N – Order of the Elliptic Curve Points
m_1, m_2 are multiplicative prime moduli of M, and $GCD(m_1, m_2) = 1$
T – Text Message

Input: Readable message, can be given any language provided the ASCII value of the alphabet should be defined.
Output: Produce set of Elliptic Curve Points(X,Y).
Method:
Convert_Text_To_ECC_Points(T)
{
A[] = ASCII(T) // Get Ascii values of T
Set CRT Parameters M, m_1, m_2
Let $\propto [\ ] = $ empty
For each A do
$\propto [j] = A_i \ mod\ m_1$, $\propto [j+1] = A_i \ mod\ m_2$
X = Find_Max($\propto_i$) // find the largest value of $\propto_i$
For each ∝ values should be mapped with finding $P[\ ] = \propto_i \cdot G$
Create Maptable[Point,CRT_Value] = $(P[\ ], \propto_i)$
}

3.3 ECC-CRT Encryption & Decryption Process

Encryption using Elliptic curve cryptography.
Input: Set of points(X,Y) on the elliptic curve $E_P(a,b)$

Output: Set of points (X,Y) ∈ $E_P(a,b)$

Method:
ECC-CRT-Encryption(Points($P_{m_1}, P_{m_2}, \ldots . P_{m_n}$))
{
public keys of sender and receiver,
$PUB_a = n_a \times G$
$PUB_b = n_b \times G$ where n_a, n_b chosen private keys. $0 < n_a, n_b < N - 1$
let k be the chosen random variable, such that $0 < k < N - 1$.
Calculate $C_1 = k \times G$

For each pair $(P_{m_i}, P_{m_{i+1}})$ do
$C_i, C_{i+1} = \{P_{m_i} + k \times PUB_b, P_{m_{i+1}} + k \times PUB_b\}$
$C_m = C_1, C_i, C_{i+1}$, $i = 1,2, \ldots \ldots, n$
Output C_m
}

Decryption using Elliptic curve Cryptography.
Input: Set of points(X,Y) on the elliptic curve $E_P(a, b)$

Output: Set of points (X,Y) ∈ $E_P(a, b)$

Method:
ECC-CRT-Decryption(Points($C_1, C_2, \ldots\ldots, C_n$)
{
Extract key from C_1
K = $n_b \times C_1$ (where n_b is the private key of the receiver).
For every C_i, $i = 2,3, \ldots \ldots, n$
from C2 to obtain P_{m_1},
$P_{m_1} = P_{m_1} + k \times\ PUB_b - n_b \times k \times G$
$= P_{m_1} + k \times n_b \times G - n_b \times k \times G$
$= P_{m_1} + n_b \times k \times G - n_b \times k \times G = P_{m_1}$
from C3 to obtain P_{m_2}.
$P_{m_2} = P_{m_2} + k \times\ PUB_b - n_b \times k \times G$
$= P_{m_2} + k \times n_b \times G - n_b \times k \times G$
$= P_{m_2} + n_b \times k \times G - n_b \times k \times G = P_{m_2}$
}

3.4 Reverse Mapping of Elliptic Curve Points to Text

Reverse of points to Tamil text using Chinese Remainder Theorem.
Now calculate M from m_1 and m_2
M = (m1 X n1 X inverse(n1) + m2 X n2 X inverse(n2)) mod N, described in the following algorithm.
Input: Set of Elliptic Curve Points(X,Y)
Output:. Readable input message.
Method:
Reverse_Mapping_ECC_Points_To_Text(W)
{
Find inverse of $m_1\ mod\ m_2$ and $m_2\ mod\ m_1$;
For each point W(x,y) using Maptable find
$\propto_i = W(x, y)\ where\ W(x, y)\ equal\ to\ P(x, y)$
For a pair of ∝ values $(\propto_i, \propto_{i+1})$ do
Temp1 = $\propto_i \times\ m_1 \times {m_1}^{-1}$
Temp2 = $\propto_{i+1} \times\ m_2 \times {m_2}^{-1}$
A[i] = (Temp1 + Temp2) mod M
Get A[i] th ASCII character T_i
Combine every T_i to get the Text Message T

}

4. Message Encryption and Decryption Implementation using ECC-CRT

The implementation was done using Subline Text verson-3 on Lenovo ThinkBook laptop model with the system configuration of intel CORE i5 processor with 2.20 GHz and 16 GB Ram with 192-bit key size of NIST (National Institute of Standards and Technology) recommended for the implementation of Elliptic curve parameter. They are:

i. a = 11;
ii. b = 2455155546008943817740293915197451784769108058161191238065;
iii. p = 6277101735386680763835789423207666416083908700390324961279;
iv. nB = 28186466892849679686038856807396267537577176687436853369;
v. G={60204628237568865675821348058752611191669876636884684818, 174050332293622031404857552280219410364023488927386650641};
vi. Pb={2803000786541617331377384897435095499124748881890727495642, 4269718021105944287201929298168253040958383009157463900739};
vii. Text = “SRM Institute of Science and Technology”

4.1 Text to Elliptic Point Conversion Process

i. Input Text = “SRM Institute of Science and Technology”
ii. ASCII values of the input = [83, 82, 77, 32, 73, 110, 115, 116, 105, 116, 117, 116, 101, 32, 111, 102, 32, 83, 99, 105, 101, 110, 99, 101, 32, 97, 110, 100, 32, 84, 101, 99, 104, 110, 111, 108, 111, 103, 121]
iii. Get Maximum(ASCII input values), that is 121, then set M is greater than 121 and $M = m_1, m_2$ such that, GCD(m_1, m_2) = 1. Here M = 143
iv. Group ASCII Values according to M.
v. [5, 6, 4, 5, 12, 0, 6, 10, 8, 7, 6, 0, 11, 5, 12, 6, 1, 6, 12, 6, 0, 7, 12, 6, 10, 2, 6, 10, 7, 1, 11, 3, 6, 10, 5, 6, 8, 0, 1, 6, 10, 2, 6, 0, 8, 0, 10, 2, 6, 10, 6, 9, 6, 0, 9, 1, 6, 10, 6, 7, 10, 2, 8, 0, 0, 5, 6, 0, 7, 1, 4, 9, 7, 1, 12, 4, 4, 0]
vi. With the generator G, constructed points on elliptic curve are,
vii. Pm= [3443036292837963759546685842252818034438575132436169939548, 568215723800040768087579915035785248418187453186037543584], [4181600039257606811702445814091795515382674993670451363594, 4145864787418078582741371957294208579442183461049606472962], [5816974679166206479449678315796610621695041936087021819827, 5990665915885689608438704467746222618933646319921982157727], [3786948970427612552829445802542365824897011513834778634630, 4298963390352331878364098142582004096663285750649430704591] and so on...

4.2 Encryption Process

i. Each point considers as Pm, and encrypted as, C = kG,Pm+kPbub, where kG = (2553986348910663776233311747947521386085452801244003930239, 6054206530771321844149094895450517595579248348317492258426), and Pm+kPbub=

(4650517478818334322569896490468044831719046727403924728252,
4799912126540324155491715700097021953177600481154529961843),
(5103177365715759592064308134138930589690629186607826991365,
1961307840107939418010565929966263512444030943913685583437),
(6193199055113969152687712056392098586164011469546956708719,
3968060648383654175232669533869346046476775347528732426056),
(4650517478818334322569896490468044831719046727403924728252,
4799912126540324155491715700097021953177600481154529961843),
(1579701179631292406088991148392154677185778402116125967385,
2805267123498414860490239994873784424572054494203738930942),
(2355477037527639396321212673447711444596965044207895531821,
1943714316891614729861689740853781228872124693286185146405) and so on…

The obtained values are with respect to the selected Generator value, if the generator value is different and foe the same input text, then accordingly, we get the different ciphertext value. Also, the same for selecting different k values. This ciphertext will be sent to the receiver.

4.3 Decryption Process

i. In decryption, from kG, key is extracted, and using the extracted key Pm is obtained by,
(451578332123131726228205654874886282322320607903046191557,
3416643315589709844888130285908365692064465573445880563824),
(3511977767041722340803634309370047399223581713793412001154,
22635282023438897720799494022530414118255720611850115995),
(5008627072379688015859085641769200051967712136055683167836,
171988491142659365744790108100019648217239346159555842925),
(451578332123131726228205654874886282322320607903046191557,
3416643315589709844888130285908365692064465573445880563824),
(1267287162293117354266037246381199791649550490142650107179,
319149749247514537745477719083287431841068322622128640297),
(60204628237568865675821348058752611191669876636884684818,
174050332293622031404857552280219410364023488927386650641), and so on…

4.4 Elliptic Point to Text Conversion Process

i. From the above points, are then mapped with the values [5, 6, 4, 5, 12, 0,…..]
ii. The values are converted to the original ASCII values by [83, 82, 77, 32,……..]
iii. the corresponding ASCII character conversion, we obtain the Plain text Message as, “SRM Institute of Science and Technology”

5. Performance Evaluation

Elliptic curve cryptography algorithm is best algorithm for providing strong security even with small length keys when compared to all other asymmetric cryptographic algorithms. Now the overall complexity of the proposed algorithm is analysed and given in table.

Table 1
Overall Complexity analysis of the Proposed Algorithm

Process Module	Input size (points/text)	Time for execution (ms)	Size of the Output(points/text)
Input Text to Elliptic Curve Points	3	0.3	6
Encryption	3	1.2	7
Decryption	7	1.6	6
Elliptic Curve Points to Text Message	6	0.6	3

There are several methods exists for converting text message to elliptic curve points, used in the implementation of elliptic curve cryptography. The following table shows the comparative performance of proposed algorithm with the existing algorithms.

Table 2
Comparative Performance with existing algorithms

Algorithm References	Input size (word)	Encryption Time(ms)	Decryption Time(ms)	Look-up Table (Y/N)
[1]	1	20	30	Y
[4]	2	10.5	9.35	Y
[2]	2	10	11.7	Y
[3]	3	4.8	7.2	N
Proposed (ECC-CRT)	3	1.5	2.1	N

The following diagram shows the graphical representation of the performance of the proposed algorithm with the existing algorithms.

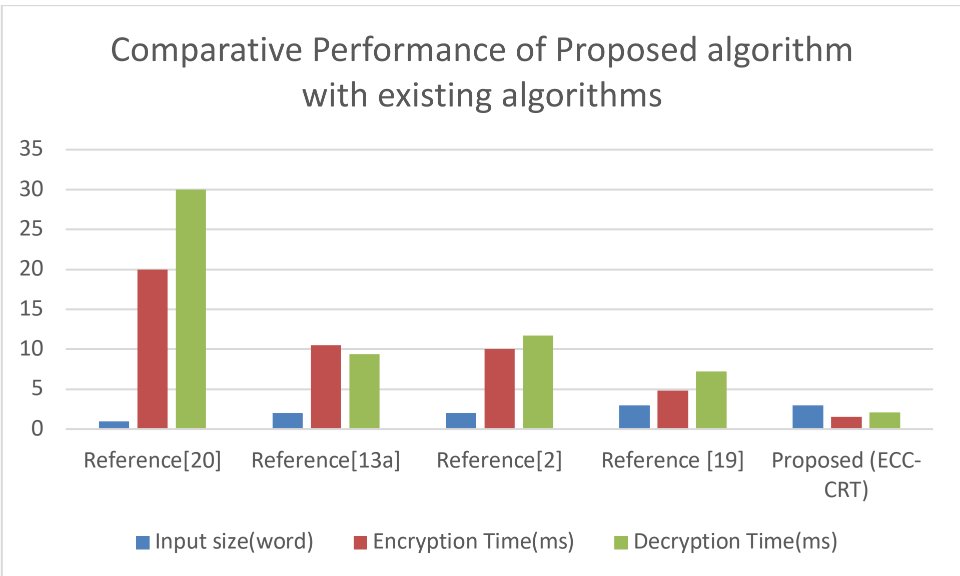

Fig. 4. Comparative Performance of Proposed algorithm with existing algorithms

The proposed ECC-CRT algorithm can be implemented in any languages whose alphabets are defined by the ASCII values, so that, the security level will be increased, also tested that, the vulnerability is very low for any cryptanalysis.

6. Conclusion

The proposed algorithm using Chinese Remainder Theorem, construct points from the text message with a smaller number of iterations from the generator point by reducing the larger values to smaller one, proved that, which reduce the time complexity of overall elliptic curve cryptographic algorithm by 40%, also proved that the strength of the security getting increased by introducing the intermediate values between the curve points and the messages.

Acknowledgement
This research was not funded by any grant.

References

[1] Ghosh, Tapas Kumar. "A Conversion Algorithm Of Text Messages Into Elliptic Curve Points." *Advances and Applications in Mathematical Sciences* 21, no. 9 (2022): 5445-5456.

[2] Das, Prasenjit, and Chandan Giri. "An efficient method for text encryption using elliptic curve cryptography." In *2018 IEEE 8th International Advance Computing Conference (IACC)*, pp. 96-101. IEEE, 2018. https://doi.org/10.1109/IADCC.2018.8692087

[3] Reyad, Omar. "Text message encoding based on elliptic curve cryptography and a mapping methodology." *Inf. Sci. Lett* 7, no. 1 (2018): 7-11. https://doi.org/10.18576/isl/070102

[4] Subrahmanyam, Rolla, N. Rukma Rekha, and YV Subba Rao. "Authenticated distributed group key agreement protocol using elliptic curve secret sharing scheme." *IEEE Access* (2023). https://doi.org/10.1109/ACCESS.2023.3274468

[5] Gowda, Bore SB. "Implementation of Elliptic Curve Cryptography over a Server-Clie| nt network." In *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, pp. 116-119. IEEE, 2020. https://doi.org/10.1109/ICDCS48716.2020.243562

[6] Menandas, J. Josepha, and Mary Subaja Christo. "The Revelation of Tamil Cryptographic Lexicon–Connecting Tamil Characteristics and Cubic Curve." In *2023 International Conference on Networking and Communications (ICNWC)*, pp. 1-6. IEEE, 2023. https://doi.org/10.1109/ICNWC57852.2023.10127454

[7] Christo, Mary Subaja, V. Elizabeth Jesi, Uma Priyadarsini, V. Anbarasu, Hridya Venugopal, and Marimuthu Karuppiah. "Ensuring improved security in medical data using ecc and blockchain technology with edge devices." *Security and Communication Networks* 2021 (2021): 1-13. https://doi.org/10.1155/2021/6966206

[8] Rasina Begum, B., and P. Chitra. "ECC-CRT: an elliptical curve cryptographic encryption and Chinese remainder theorem based deduplication in cloud." *Wireless Personal Communications* 116, no. 3 (2021): 1683-1702. https://doi.org/10.1007/s11277-020-07756-7

[9] Freeda, J., and J. Josepha menandas. "IoT Based Innovation Schemes in Smart Irrigation System with Pest Control." In *Emerging Trends in Computing and Expert Technology*, pp. 657-669. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-32150-5_64

[10] Sengupta, Aritro, and Utpal Kumar Ray. "Message mapping and reverse mapping in elliptic curve cryptosystem." *Security and Communication Networks* 9, no. 18 (2016): 5363-5375. https://doi.org/10.1002/sec.1702

[11] Reyad, Omar. "Text message encoding based on elliptic curve cryptography and a mapping methodology." *Inf. Sci. Lett* 7, no. 1 (2018): 7-11. https://doi.org/10.18576/isl/070102

[12] Agrawal, Komal, and Anju Gera. "Elliptic curve cryptography with hill cipher generation for secure text cryptosystem." *International journal of computer applications* 106, no. 1 (2014).

[13] Reyad, Omar. "Text message encoding based on elliptic curve cryptography and a mapping methodology." *Inf. Sci. Lett* 7, no. 1 (2018): 7-11. https://doi.org/10.18576/isl/070102

[14] Zainal, Salbiah, Rasimah Che Mohd Yusoff, Hafiza Abas, Suraya Yaacub, and Norziha Megat Zainuddin. "Review of design thinking approach in learning IoT programming." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 28-38.

[15] Razali, Rozita, and Syuhaida Ismail. "Benchmarking for Industry Centre of Excellence (ICoE) at Majlis Amanah Rakyat (MARA) Technical and Vocational Education and Training (TVET) Institutions." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 7-19.

[16] Amir, Muhamad Arshad Mohamad, and Faizah Mohamad Nor. "Excellent English teachers–a view from English teachers." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 20-27.
[17] Veza, Ibham, Mohd Farid Muhamad Said, Tri Widodo Besar Riyadi, Mohd Azman Abas, and Zulkarnain Abdul Latiff. "Issues in the Science and Engineering Education in Indonesia: How to Improve Competitiveness Through STEM Mastery." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 1-6.
[18] Zhai, Xiujun, A. Rajaram, and K. Ramesh. "Cognitive model for human behavior analysis." *Journal of Interconnection Networks* 22, no. Supp04 (2022): 2146013. https://doi.org/10.1142/S0219265921460130
[19] Arulselvan, G., and A. Rajaram. "Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs." *Journal of Intelligent & Fuzzy Systems* Preprint (2023): 1-16. https://doi.org/10.3233/JIFS-231905
[20] Ilakkiya, N., and A. Rajaram. "Blockchain-assisted secure routing protocol for cluster-based mobile-ad hoc networks." *International Journal of Computers Communications & Control* 18, no. 2 (2023). https://doi.org/10.15837/ijccc.2023.2.5144
[21] Joseph, Shajan, and A. Rajaram. "Efficient secure and fair cluster routing protocol: An improved bee colony optimization cluster based efficient secure and fair routing protocol for mobile ad hoc network." *Journal of Computational and Theoretical Nanoscience* 14, no. 7 (2017): 3503-3509. https://doi.org/10.1166/jctn.2017.6535